UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/541,510	07/18/2007	Gilles Merle	274880US2PCT	3879

22859   7590   03/23/2011
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
TOLENTINO, RODERICK

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
03/23/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)
	10/541,510	MERLE ET AL.
	Examiner	Art Unit	
	Roderick Tolentino	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _13 January 2011_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-38_ is/are pending in the application.

    4a) Of the above claim(s) _1-19_ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _20-38_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _18 July 2007_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 20 – 38 are pending.

Response to Arguments

2.   Applicant's arguments with respect to claim 20 have been considered but are

moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 20 – 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Harada et al. U.S. PG-Publication No. (2003/0007640) in view of Montgomery U.S. PG-

Publication No. (2002/0141590).

5.   As per claim 20, Harada teaches at a transmission, each block of a family is

scrambled by a key associated with the family, (Harada, Paragraph 0192, data divided

into blocks then encrypted and unique key encrypts each block) and at a reception,

each block of a family is descrambled by the key associated with the family (Harada,

Paragraph 0008, decryption unit) but fails to teach defined as a function of a specific

processing capacity and a level of security of the respective deciphering modules.

However, in an analogous art Montgomery teaches defined as a function of a specific

processing capacity and a level of security of the respective deciphering modules

(Montgomery, Paragraphs 0035 and 0037, key length determines desired level of

security).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Montgomery's apparatus for streaming data using rotating

cryptographic keys with Harada's digital work protection system record/playback device

because it offers the advantage of further secure transmission of digital data

(Montgomery, Paragraph 0012).

6.   As per claim 21, Harada teaches the descrambling modules are different

peripheral elements associated with the receiver terminal (Harada, Paragraph 0079,

transmit data to a phone).

7.   As per claim 22, Harada teaches the descrambling modules comprise different

algorithms (Harada, Paragraph 0008, decryption unit).

8.   As per claim 23, Harada teaches the descrambling modules comprise identical

algorithms (Harada, Paragraph 0008, decryption unit).

9.   As per claim 24, Harada teaches the data to be distributed are in a form of a

previously stored file (Harada, Paragraph 0080, digital file on server ready for

distribution).

10.   As per claim 25, Harada teaches the data to be secured are in a form of a

broadcast or downloaded stream and processed in real time by the terminal (Harada,

Paragraph 0080, digital file on server ready for distribution).

11.   As per claim 26, Harada teaches a duration of use of the stream is divided into

crypto periods, each corresponding to a descrambling key, and wherein prior to each

start of the crypto period a message is inserted into the stream so as to warn the

descrambling module of the change in crypto period (Harada, Paragraph 0008,

decryption unit).

12.   As per claim 27, Harada teaches the message comprises all information

necessary for descrambling the stream utilized during the following crypto period

(Harada, Paragraph 0008, decryption unit).

13.   As per claim 28, Harada teaches the data represent audio and/or video programs

protected by a DRM system (Harada, Paragraph 0080, digital file on server ready for

distribution).

14.   As per claim 29, Harada teaches the data represent images synthesis or anime

drawings (Harada, Paragraph 0080, digital file on server ready for distribution, anime

drawings are merely intended use).

15.   As per claim 30, Harada teaches subdivide the data into M distinct families of N

blocks; assign each family a specific identification parameter associated and scramble

each block by a key in biunivocal relation with the parameter (Harada, Paragraph 0192,

data divided into blocks then encrypted and unique key encrypts each block), and a

descrambling platform comprising identify the family of each block so as to descramble

each block of a family by the descrambling module corresponding to the parameter

(Harada, Paragraph 0008, decryption unit) but fails to teach with at least one

descrambling module having a specific processing capacity and a specific level of

security. However, in an analogous art Montgomery teaches with at least one descrambling module having a specific processing capacity and a specific level of security (Montgomery, Paragraphs 0035 and 0037, key length determines desired level of security).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Montgomery's apparatus for streaming data using rotating cryptographic keys with Harada's digital work protection system record/playback device because it offers the advantage of further secure transmission of digital data (Montgomery, Paragraph 0012).

16.   As per claim 31, Harada teaches the descrambling modules are distinct peripherals associated with the receiver terminal (Harada, Paragraph 0080, transmit data to a phone and decrypted by the phone).

17.   As per claim 32, Harada teaches subdivide the stream into M distinct families of N blocks, assign each family a specific identification parameter associated (Harada, Paragraph 0008, decryption unit), define for each module a key as a function of the processing capacity and a degree of security; and scramble each block belonging to a family by a key in biunivocal relation with the parameter (Harada, Paragraph 0192, data divided into blocks then encrypted and unique key encrypts each block) but fails to teach with at least one descrambling module having a specific processing capacity and a specific level of security. However, in an analogous art Montgomery teaches with at least one descrambling module having a specific processing capacity and a specific

level of security(Montgomery, Paragraphs 0035 and 0037, key length determines desired level of security).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Montgomery's apparatus for streaming data using rotating cryptographic keys with Harada's digital work protection system record/playback device because it offers the advantage of further secure transmission of digital data (Montgomery, Paragraph 0012).

18.   As per claim 33, Harada teaches identifying the family of each block so as to descramble each block of a family by the descrambling module corresponding to the parameter (Harada, Paragraph 0192, data divided into blocks then encrypted and unique key encrypts each block).

19.   As per claim 34, Harada teachesa plurality of distinct descrambling modules each identified by the specific identification parameter (Harada, Paragraph 0008, decryption unit).

20.   As per claim 35, Harada teaches the receiver terminal is a PDA and one of the descrambling modules is integrated into the PDA, and at least a second descrambling module is a smart card of SIM type connected to the PDA (Harada, Paragraph 0080, phone with memory card).

21.   As per claim 36, Harada teachesfor securing a video-on-demand service (VOD) (Harada, Paragraph 0080, music on demand).

22.   As per claim 37, Harada teachesfor securing a music-on-demand service (MOD) (Harada, Paragraph 0080, music on demand).

23.   As per claim 38, Harada teachesfor securing access to a broadcast service for

electronic books either online or downloaded from portable media (Harada, Paragraph

0080, digital work to a mobile phone).

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Roderick Tolentino whose telephone number is (571)

272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Edan Orgad can be reached on (571) 272-3811. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/   Roderick Tolentino
Primary Examiner, Art Unit 2439   Examiner
                                                         Art Unit 2439

/R. T./
Examiner, Art Unit 2439